公告本

I279150

發明專利說明書

（填寫本書件時請先行詳閱申請書後之申請須知，作※記號部分請勿填寫）

※ 申請案號：91135435 ※IPC分類：H04Q7/32(2006.01)

※ 申請日期：91、12、6.

壹、發明名稱

(中文) 混合通訊網路之鑑認

(英文) AUTHENTICATION IN A HYBRID COMMUNICATIONS NETWORK

貳、發明人（共 5 人）

發明人 1 （如發明人超過一人，請填**說明書發明人續頁**）

姓名：(中文) 尤拉姆 里莫米

(英文) YORAM RIMONI

住居所地址：(中文) 以色列海法市克倫哈耶蘇街10號

(英文) 10 KEREN HAYESOD STREET, HAIFA 31999, ISRAEL

國籍：(中文) 以色列 (英文) ISRAEL

參、申請人（共 1 人）

申請人 1 （如申請人超過一人，請填**說明書申請人續頁**）

姓名或名稱：(中文) 美商奎康公司

(英文) QUALCOMM INCORPORATED

住居所或營業所地址：(中文)美國加州聖地牙哥市摩豪斯大道5775號

(英文) 5775 MOREHOUSE DRIVE, SAN DIEGO, CALIFORNIA 92121-1714, U.S.A.

國籍：(中文) 美國 (英文) U.S.A.

代表人：(中文) 菲力普 R. 華德斯

(英文)PHILIP R. WADSWORTH

說明書發明人續頁

發明人 2

姓名：(中文) 亞里詹洛 R. 后克曼

(英文) ALEJANDRO R. HOLCMAN

住居所地址：(中文) 美國加州聖地牙哥市迪芳夏道1054號

(英文) 1054 DEVONSHIRE DRIVE, SAN DIEGO, CALIFORNIA 92107, U.S.A.

國籍：(中文) 美國 (英文) U.S.A.

發明人 3

姓名：(中文) 麥克 葛林

(英文) MICHAEL GREEN

住居所地址：(中文) 以色列希克倫亞克夫市耶福諾夫街9號

(英文) 9 YAFE NOF STREET, ZICHRON YAAKOV 30900, ISRAEL

國籍：(中文) 以色列 (英文) ISRAEL

發明人 4

姓名：(中文) 尼克海 顏

(英文) NIKHIL JAIN

住居所地址：(中文) 美國加州聖地牙哥市費德曼道4291號

(英文) 4291 FEDERMAN LANE, SAN DIEGO, CALIFORNIA 92130, U.S.A.

國籍：(中文) 印度 (英文) INDIA

發明人 5

姓名：(中文) 安德魯 T. 杭特

(英文) ANDREW T. HUNTER

住居所地址：(中文) 美國加州聖地牙哥市郵政信箱910023號

(英文) P.O. BOX 910023, SAN DIEGO. CALIFORNIA 92191, U.S.A.

國籍：(中文) 英國 (英文) UNITED KINGDOM

捌、聲明事項

☐ 本案係符合專利法第二十條第一項☐第一款但書或☐第二款但書規定之期間，其日期為：＿＿＿＿＿＿＿＿

☑ 本案已向下列國家（地區）申請專利，申請日期及案號資料如下：

【格式請依：申請國家（地區）；申請日期；申請案號　順序註記】

1.美國；2001年12月07日；60/340,172

2.美國；2002年01月17日；60/350,401

3.美國；2002年02月14日；10/077,651

4.美國；2002年02月19日；60/358,471

☑ 主張專利法第二十四條第一項優先權：

【格式請依：受理國家（地區）；日期；案號　順序註記】

1.美國；2001年12月07日；60/340,172

2.美國；2002年01月17日；60/350,401

3.美國；2002年02月14日；10/077,651

4.美國；2002年02月19日；60/358,471

5.

6.

7.

8.

9.

☐ 主張專利法第二十五條之一第一項優先權：

【格式請依：申請日；申請案號　順序註記】

1.

2.

3.

☐ 主張專利法第二十六條微生物：

☐國內微生物　【格式請依：寄存機構；日期；號碼　順序註記】

1.

2.

3.

☐國外微生物　【格式請依：寄存國名；機構；日期；號碼　順序註記】

1.

2.

3.

☐熟習該項技術者易於獲得，不須寄存。

玖、發明說明

(發明說明應敘明：發明所屬之技術領域、先前技術、內容、實施方式及圖式簡單說明)

發明背景

I. 技術領域

本發明係廣泛關於在不同細胞式通訊系統中之鑑認方法及裝置。

II. 先前技術

所謂的分碼多向近接(code division multiple access；CDMA)調變技術僅僅是用於促進大量系統使用者之通訊的數種技術之一。雖然也可使用其他技術(例如，分時多向近接(time division multiple access；TDMA)、分頻多向近接(frequency division multiple access；FDMA)、如振幅對信號側頻段(amplitude companded single sideband；ACSSB)調變之類的AM調變原理)，但是CDMA的優點顯然優於其他調變技術。下列美國專利已發表在多向近接通訊系統中使用CDMA技術：美國專利案號4,901,307，標題為"Spread Spectrum Multiple Access Communication System Using Satellite Or Terrestrial Repeaters"，該專利已讓渡給本受讓人，其內容以引用方式併入本文。

在美國專利案號4,901,307中發表一種多向近接技術，其中大量行動電話系統使用者(每個使用者都具有收發器)使用分碼多向近接(code division multiple access；CDMA)展頻通訊信號，以透過衛星中繼器(repeater)或地面通訊基地台(也稱為單元基地台(cell base station)或基地台(cell-site))。使用CDMA通訊時，會多次重複利用頻譜，因此能夠增加

系統使用者容量。CDMA技術之運用所達成的光譜效率高於使用其他多向近接技術。

在傳統行動電話系統中，可用的頻率頻段被分割成頻道(頻寬通常是30 KHz)，同時使用FM調變技術。系統服務區域在地理上被分割成不同大小的單元(cell)。可用的頻率頻道被分割成數組，每組通常包含相等數目的頻道。頻率組被指派給單元，以使同等頻道(co-channel)干擾的可能性降至最低限度。例如，考慮到有七組頻率組且單元是相等大小之六邊形的系統。一個單元中使用的一組頻率組不會被用在六個最接近或周圍鄰接的單元中。另外，一個單元中使用的該組頻率組不會被用在十二個次要最接近鄰接的單元中。

在傳統細胞式通訊系統中，所實施之交遞的作用為，當行動台橫跨單元邊界時，能夠持續呼叫或其他類型連接(即，資料鏈路)。當處理呼叫或連接的單元基地台通知從行動台所接收的信號強度下降至預先決定限定值以下時，就會起始從某單元交遞至另一單元。低信號強度指示意謂著行動台必定在單元邊界附近。當信號位準下降至預先決定限定值以下時，基地台要求系統控制器決定鄰近基地台接收行動台信號的信號強度是否比目前基地台接收的信號強度更強。

系統控制器響應目前基地台的詢問，而將具有交遞要求的訊息傳送至鄰近基地台。鄰近於目前基地台的基地台採用特殊掃描接收器，用於在指定頻道尋找該行動台的信

號。萬一鄰近基地台將足夠的信號位準回報給系統控制器，則會嘗試交遞。

接著，當從新基地台中使用的頻道集選取閒置頻道時，則會起始交遞。一控制訊息被傳送至該行動台，以命令該行動台從目前頻道切換至新頻道。同時，系統控制器將呼叫從第一基地台切換至第二基地台。

在傳統系統中，如果交遞至新基地台失敗，則會中斷呼叫。有許多原因會造成交遞失敗。如果鄰近單元中沒有可用於呼叫通訊的閒置頻道，就會發生交遞失敗。如果另一基地台報告其收訊到(hearing)討論中行動台，實際上，這個基地台事實上係在完全不同的單元中使用相同的頻道而收訊到不同行動台時，也會發生交遞失敗。這項報告錯誤會導致呼叫被切換至錯誤的單元，通常是信號強度不足以維持通訊的單元。另外，萬一行動台無法收訊到頻道切換命令，就會發生交遞失敗。實際的操作經驗指出，經常發生交遞失敗令人質疑系統可靠度。

傳統電話系統中另一項常見問題發生於，當行動台在兩個單元之間的邊界時。在此情況下，信號位準傾向於在兩個基地台波動。這項信號位準波動導致"乒乓球"(ping-ponging)狀況，其中會提出重複的要求，以在兩個基地台之間來回處理呼叫。此類額外的非必要交遞要求會增加行動台錯誤收訊到頻道切換命令的可能性，或根據無法收訊到命令。另外，如果不慎將呼叫轉遞至目前所有頻道皆在使用中而無法接受交遞的單元，則乒乓球狀況會引發

呼叫中斷的可能性。

下列美國專利已發表在交遞期間，透過一個以上單元為行動台提供通訊之方法及系統：美國專利案號5,101,501，標題為"Method And System For Providing A Soft Handoff In Communications In A CDMA Cellular Telephone System"，該專利已讓渡給本受讓人，其內容以引用方式併入本文。在此環境中，藉由從相對應於行動台離開之單元的基地台到相對應於行動台進入之單元的基地台的最終交遞，促使細胞式通訊系統內的通訊不會被中斷。在單元基地台與行動台之間的通訊中(其中兩個或兩個以上基地台或基地台扇區同時傳輸行動台)，此類型交遞被視為"軟"交遞。經證實發現使用此類"軟"交遞可實質上降低在一對基地台之間提出重複交遞要求之乒乓球狀況的發生率。

下列美國專利已發表改良型交遞 技術：美國專利案號5,267,261，標題為"Mobile Station Assisted Soft Handoff In A CDMA Cellular Communications System"，該專利已讓渡給本受讓人，其內容以引用方式併入本文。改良軟交遞技術的方式為，在行動台量測系統每個基地台所傳輸之"前導"信號的強度。這些前導強度測量屬於對軟交遞處理程序的協助，其方式為促進可實行之基地台交遞候選之識別。

改良型軟交遞技術規定，行動台監視來自鄰近基地台的前導信號強度。當所量測信號強度超過既定限定值時，行動台經由正在與行動台通訊的基地台，將一信號強度訊息傳送至系統控制器。從系統控制器傳至新基地台及傳至行

動台的命令訊息建立透過新基地台和目前基地台的同時通訊。當行動台偵測到相對應於正在與行動台通訊之至少一基地台的前導信號強度已下降至預先決定位準以下，則行動台經由正在與行動台通訊的基地台，以向系統控制器報告相對應基地台的所量測信號強度指示。從系統控制器傳至所識別基地台及傳至行動台的命令訊息終止透過相對應基地台通訊，同時透過其他基地台繼續通訊。

雖然前述的技術非常適用於同一細胞式通訊系統單元之間的呼叫轉遞，但是當行動台移動至另一細胞式通訊系統之基地台所服務的單元時，則會出現更困難的情況。在此類「系統間」交遞的一項複雜因素為，鄰近細胞式通訊系統通常具有互異的特性。例如，鄰近細胞式通訊系統通常係以不同頻率運作，並且可維持不同位準的基地台輸出功率或前導信號強度。這些差異實際上會妨礙行動台執行前導信號強度比較，並且如同現有行動台協助型軟交遞技術的考量。

當無法取得資源來處理系統間軟交遞時，如果要維持無中斷服務，則系統間之呼叫或連接的交遞時序變成非常關鍵。也就是說，系統間交遞的執行時機必須很可能導致在系統間成功轉遞呼叫或連接。在此一交遞中(本文中稱為硬交遞)，介於行動台與一系統之間的通訊必須先終止，之後才能開始介於行動台與其他系統之間的通訊。例如，只有在下列情況下才能嘗試交遞：

(i) 新單元中有可用的閒置頻道；

(ii) 行動台實際上在新單元基地台範圍內，但是在失去與目前單元基地台的聯繫之前；以及

(iii) 行動台所在的位置確信接收到頻道切換命令。

在理想情況下，每個此類系統間硬交遞的處理方式為，使介於不同系統之基地台間之"乒乓球"交遞要求的可能性降至最低限度。但是，由於現有交遞程序無法確定何時，及透過哪些基地台，應該為行動台提供新的頻率及頻道資訊，以及指示轉遞現有呼叫或連接，所以極為困難。

現有系統間交遞技術的這些及其他缺點會降低細胞式通訊的品質，並且由於不能同時接收細胞式通訊系統繼續傳播，所以預期會進一步降低效能等級。於是，需要有一種系統間交遞技術，其能夠可靠地引導介於不同細胞式通訊系統之基地台間之呼叫或連接的交遞。

下列美國專利已發表一種用於執行介於第一與第二細胞式通訊系統之基地台間通訊之系統間交遞的方法及系統：美國專利案號5,697,055，標題為"Mobile Station Assisted Soft Handoff In A CDMA Cellular Communications System"，該專利已讓渡給本受讓人，其內容以引用方式併入本文。在行動台，量測第二系統之第二基地台所傳輸之信號的可計量參數。當所量測之可計量參數值通過第一預先決定位準時，行動台經由第一系統的第一基地台將一信號品質訊息傳達至第一行動交換控制台。

接著，將一頻道要求訊息從該第一行動交換控制台傳達至第二系統內的第二行動交換控制台。在第二基地台上，

也會量測從行動台接收之信號的可計量參數。當所量測的可計量參數值通常預先決定位準時，第二基地台建立與行動台之間的通訊。或者，在行動台上量測第一基地台所傳輸之第一前導信號的信號強度。接著，當所量測之第一前導信號的信號強度低於第二預先決定位準時，則會將一交遞要求訊息傳送至第二基地台，藉以建立基地台通訊。介於行動交換控制台間之語音鏈路之提供係考慮到在第一與第二細胞式通訊系統之間轉遞現有連接，並且促進系統間軟交遞的效能。

雖然這項配置非常適用於雙方系統都是CDMA架構且因此能夠執行軟交遞之情況，但是仍然有如何處理系統間交遞的問題，其中系統中的一或多個系統無法執行此交遞。例如，所謂的GSM標準不具有軟交遞機制。因此，在使用從CDMA網路到GSM網路之空氣介面的呼叫交遞過程中會有問題。另外，由於CDMA 2000機制無法轉遞執行GSM鑑認所需的資料，所以無法完成GSM鑑認。GSM中之加密不同於CDMA 2000中之加密。

解決此項問題的一種方式為，修改GSM以能夠實行交遞至非GSM系統，例如，CDMA系統。然而，GSM創建已有多年時間，相對而言，業者無意願花大筆金額來修改現有設備，以接受鄰近不相容的系統。如果將新訊息加入至支援雙模式行動台的空間介面，則必須修改以支援這些新訊息。顯而易見，就業者的立場而言，這不是所期望的形式。

介於CDMA系統與GSM系統間之交遞的另一項問題為，

CDMA和GSM鑑認係使用兩種不同的方法及金鑰。GSM與CDMA 1X的鑑認方法基本上相同，但是金鑰具有不同大小。CDMA 1X具有額外的程序，例如，唯一質問及計數(unique challenge and count)方法，分別用於防止頻道攔截及重播攻擊。

發明內容

本發明解決前面提出的問題。

根據本發明一項觀點，本發明揭示一種鑑認一行動台之方法，其中該行動台係從一由第一細胞式通訊系統中之第一行動交換控制台所控制之第一基地台移動至一由第二、不同之細胞式通訊系統中之第二行動交換控制台所控制之第二基地台，該方法包括：在該第二細胞式通訊系統產生一鑑認碼，其中產生之該鑑認碼是將一演算法套用至一指派給該等第細胞式通訊系統之該行動台的私鑰及該第二細胞式通訊系統產生之一亂數的結果；在該第一細胞式通訊系統產生一鑑認碼，其中產生之該鑑認碼是將一演算法套用至該私鑰及該亂數的結果；在一資料封包中，將在該第一細胞式通訊系統產生之該鑑認碼傳輸至一行動台；將在該第一細胞式通訊系統產生之該鑑認碼從該行動台傳輸至該第二細胞式通訊系統；以及將在該第一細胞式通訊系統產生的該鑑認碼比對於在該第二細胞式通訊系統產生的該鑑認碼。

從下文中參考附圖解說的本發明示範性具體實施例詳細說明，將可更明白隨附申請專利範圍中之特徵所提出的

本發的前述和進一步功能及其優點。

圖式簡單說明

圖式中：

圖1顯示細胞式通訊系統的原理表示圖；

圖2顯示介於兩個細胞式通訊系統之間邊界的原理表示圖；

圖3顯示雙模式行動台的原理圖；

圖4顯示GSM系統中資料交換的原理表示圖；以及

圖5顯示單一模式行動台的原理圖。

本發明具體實施例詳細說明

圖1顯示示範性行動電話系統的原理圖。圖中所示的系統可利用任何多向近接調變技術，用以促進介於通常是大量系統行動台或行動電話與基地台之間的通訊。此類多向近接通訊系統技術包括：分時多向近接(time division multiple access；TDMA)、分頻多向近接(frequency division multiple access；FDMA)、分碼多向近接(code division multiple access；CDMA)及如振幅對信號側頻段(amplitude companded single sideband)調變之類的AM調變原理。例如，前面提及之美國專利案號4,901,307中發表之CDMA展頻調變技術的優點顯然優於其他多向近接通訊系統調變技術，因此是較佳調變技術。

在典型的CDMA系統中，每個基地台都會傳輸一唯一前導信號，其包含在相對應前導頻道上傳輸"前導載波"。前導信號是一種未經調變、直接序列、展頻信號，並且每個

基地台都會隨時使用通用偽隨機雜訊(pseudorandom noise；PN)擴展碼傳輸前導信號。除了提供相干(coherent)解調變的相位參考及交遞決策中使用之信號強度量測的參考以外，前導信號還允許基地台獲取起始系統同步化(即，時序)。每個基地台所傳輸的前導信號通常可能是相同的PN擴展碼，但是具有不同的編碼相位偏移量。

在圖1所示的系統中，系統控制器和交換機10(也稱為行動交換中心(MSC))通常包含影像及處理電路(圖中未顯示)，用於提供對複數個基地台12、14和16的系統控制。控制器10也控制從公共交換電話網路(PSTN)到適當基地台的路徑選擇，用以傳輸至適當的行動台。控制器10也控制從行動台，經由至少一基地台到PSTN的路徑選擇。控制器10可經由適當的基地台以導向介於行動使用者之間的呼叫，這是由於此類行動台通常不能互相直接通訊。

可藉由各種方法(例如，專用電話線路、光纖鏈路或藉由圖1所示的微波通訊鏈路)將控制器10耦合至基地台，圖1中顯示三種此類示範性基地台12、14和16及示範性行動台18(其包含行動電話)。箭頭20a和20b定義介於基地台12與行動台18之間的可能通訊鏈路。箭頭22a和22b定義介於基地台14與行動台18之間的可能通訊鏈路。箭頭24a和24b定義介於基地台16與行動台18之間的可能通訊鏈路。

基地台服務區域或單元(cell)的地理形狀經過設計，以使行動台通常最接近某基地台。當行動台處於待機狀態(即，沒有進行中的呼叫)時，行動台會持續監視來自每個

附近基地台的前導信號傳輸。如圖1所示，基地台12、14和16分別在通訊鏈路20b、22b和24b上，將前導信號傳輸至行動台18。接著，行動台藉由比較從這些特定基地台所傳輸的前導信號強度，以判斷其位於哪一個單元中。

在圖1所示的實例中，行動台18被認為最接近基地台16。當行動台18起如呼叫時，會將控制訊息傳輸至最接近的基地台，此處為基地台16。基地台16接收到呼叫要求訊息後，隨即向系統控制器10發出信號並且轉遞呼叫號碼。接著，系統控制器10透過PSTN以將呼叫連接到預定的接收者。

萬一在PSTN內起始呼叫，則控制器10會將呼叫資訊傳輸至區域中的所有基地台。接著，基地台將一傳呼訊息傳輸給預定的接收方行動台。當行動台收訊到傳呼訊息時，則會以一傳輸至最接近基地台的控制訊息回應。控制訊息向系統控制器發出信號，以通知這個特定基地台正在與行動台通訊。然後，控制器10透過最接近的基地台將呼叫投送至行動台。

當行動台18移動至起始基地台(即，基地台16)的覆蓋範圍以外時，則會藉由透過另一基地台投送呼叫，以嘗試使呼叫持續。在交遞處理程序中，有不同方法起始呼叫交遞或透過另一基地台投送呼叫。

在基地台起始型交遞方法中，起始基地台(基地台16)注意到行動台18所傳輸的信號已下降至特定限定位準。接著，基地台16將一交遞要求傳輸至系統控制器10，用於將

要求中繼至基地台16的所有鄰接基地台12、14。控制器傳輸型要求包括與頻道相關的資訊，包含行動台18使用的PN碼序列。基地台12和14將接收器調整至行動台所使用的頻道，並且測量信號強度(通常使用數位技術)。如果基地台12和14接收器之一回報的信號強度高於起始基地台回報的信號強度，則會交遞至該基地台。

或者，行動台本身可起始所謂的行動台協助型交遞。基地台都會傳輸前導信號，除了別的作用以外，其用於識別基地台。行動台配備搜尋接收器，其除了執行其他功能以外，還用於掃描鄰接基地台12和14的前導信號傳輸。如果經證實發現鄰接基地台12和14之一的前導信號強度高於既定限定值，則行動台18會將這項結果的訊息傳輸至基地台16。

接著，介於行動台與基地台之間的互動式處理程序准許行動台透過基地台12、14和16中的一或多個行動台進行通訊。在這項處理程序期間，行動台識別及測量所接收之前導信號的信號強度。這項資訊係經由正在與行動台通訊的基地台傳達至MSC。MSC在接收到這項資訊之後，隨即起始或終止介於行動台與基地台之間的連接，藉此使行動台協助型交遞生效。

前述的處理程序也被識為"軟"交遞，因為行動台同時透過一個以上基地台通訊。在軟交遞期間，MSC可組合或選取從每個基地台接收到的信號，其中這些基地台係行動台在不同單元之間移動期間正在與行動台通訊的基地台。在

相似方式中，MSC可將信號從PSTN中繼至正在與行動台通訊的每個基地台。如果行動台位於不屬於相同細胞式通訊系統(即，不是被相同MSC控制)之兩個或兩個以上基地台的覆蓋範圍內，則行動台協助型交遞傾向於更複雜。

現在將參考圖2來說明在屬於不同系統的基地台之間執行交遞的一項做法，圖中呈現細胞式通訊網路30的原理圖，其中包含受CDMA行動交換中心MSCc控制的CDMA細胞式通訊系統(例如，IS-95 1X)，及受GSM行動交換中心MSCg控制的GSM細胞式通訊系統。在圖2中，描繪出五個示範性基地台B1A至B5A分別位於CDMA系統的單元C1A至C5A內，以及五個示範性基地台B1B至B5B分別位於GSM系統的單元C1B至C5B內。雖然基於圖解便利性，圖式中將單元C1A至C5A和C1B至C5B描繪成圓形，但是應明白，單元通常被設計成其他形狀，並且實際上的形狀取決於所在區域中的地勢和地形。下文中可將單元C1A至C3A和C1B至C3B稱為"邊界"單元，因為這些單元接近介於第一與第二細胞式通訊系統之間的邊界。這項命名允許將每個系統內的其餘單位稱為"內部"單元。

接下來的說明內容係有關於一種行動台，其能夠接收及回應來自CDMA和GSM細胞式通訊系統內之基地台的信號。然而，預期可使用任何類型的通訊系統，例如，CDMA One、CDMA2000、CDMA 2000 1x、CDMA 2000 3x、高資料傳輸率原理(High Data Rate Principles；HDR)、CDMA 1xEV、CDMA 1xEVDO、TDMA、TDSCDMA、W-CDMA、GPRS及其他通訊系

統。為此目的，所組態的行動台配備雙頻帶收發器，其具有可調諧至屬於兩種細胞式通訊系統之不同操作頻率的接收鏈。附圖的圖3顯示此一行動台的原理圖。如圖所示，行動台40包含一天線42，其透過雙工器(diplexer)44連接至CDMA傳輸和接收鏈46及GSM傳輸和接收鏈48。傳輸/接收鏈46、48是各自CDMA和GSM系統的傳統傳輸/接收鏈。傳輸/接收鏈將經過適當解調變和轉換的資料輸出至常規基頻帶電路50，並且接收從基頻帶電路40傳輸的資料。傳輸/接收鏈46、48係由控制器52控制，其作用之一是在這兩個傳輸/接收鏈之間切換，以響應來自CDMA或GSM系統的控制信號。因此在本具體實施例中，這兩個傳輸/接收鏈不會同時處於作用中狀態。在另一具體實施例中，這兩個傳輸/接收鏈可同時處於作用中狀態。

在另一具體實施例中，所組態的行動台配備單一收發器，其具有可調諧至兩種細胞式通訊系統之一的接收鏈。附圖的圖5顯示此一行動台的原理圖。如圖所示，其中行動台53包含一天線54。雙工器55被連接至CDMA傳輸和接收鏈56(如果行動台是CDMA手機)。否則，行動台53被連接到GSM傳輸和接收鏈57。傳輸/接收鏈56、57是各自CDMA和GSM系統的傳統傳輸/接收鏈。傳輸/接收鏈將經過適當解調變和轉換的資料輸出至常規基頻帶電路58，並且接收從基頻帶電路58傳輸的資料。傳輸/接收鏈(56或57)係由控制器59控制。

請參閱圖2，CDMA行動交換中心(MSCc)控制從公共交換

電話網路(PSTN)到適當基地台B1A至B5A之電話呼叫的路徑選擇，用以傳輸至指定的行動台。CDMA行動交換中心MSCc也控制從位於第一細胞式通訊系統覆蓋範圍內之行動台，經由至少一基地台到PSTN之呼叫的路徑選擇。GSM行動交換中心MSCg以相似方式運作，用以管理基地台B1B至B5B的運作，以及用以在PSTN與GSM細胞式通訊系統之間投送呼叫。控制訊息等等係透過系統間資料鏈路34以在MSCc與MSCg之間傳達。

當行動台係位於CDMA系統的內部單元內時，行動台通常被程式規劃以監視從每個附近(即，內部及(或)邊界)基地台的前導信號傳輸。接著，行動台藉由比較從周圍基地台所傳輸的前導信號強度，以判斷其位於哪一個內部單元中。例如，當行動台接近內部單元邊界時，會以前面提及之美國專利案號5,267,261中說明的方法來起始行動台協助型交遞。

當行動台位於邊界單元C1A至C3A或C1B至C3B之一範圍內時，則有不同的情況發生。舉例而言，考慮到行動台位於單元C2A範圍內，但是正在接近單元C2B。在此情況下，行動台會開始從基地台B2B接收可用的信號位準，接著向基地台B2B和任何其他基地台報告行動台目前正在通訊中。藉由量測所接收信號的一或多個可計量參數(例如，信號強度、雜訊比、訊框擦除率、位元錯誤率及(或)相對時間延遲)，可決定行動台或基地台接收可用信號位準的時間。這項機制類似於前面提及之美國專利案號

5,697,055中發表的機制。

如果雙方系統都是CDMA系統，則可使用美國專利案號5,697,055中發表的交遞機制來實行介於單元C2A與單元C2B之間的交遞。然而，由於目前沒有用於使用從CDMA網路到GSM網路之空氣介面的呼叫交遞機制，所以會有問題。由於CDMA機制無法轉遞執行GSM鑑認所需的資料，所以無法完成GSM鑑認。GSM中之加密不同於CDMA中之加密。如果將新訊息加入至支援雙模式行動台的空間介面，則必須修改以支援這些新訊息。這是不希望的情況。

這項問題的解決方案是使用通用的訊息，訊息包含能夠將行動台從CDMA網路轉遞到GSM網路的指令。通用訊息必須能夠運送實行GSM鑑認與加密所需的資料。較佳方式為，通用訊息也應支援GSM中的增補功能。換言之，所建立的GSM通訊協定必須維持不變，以至於對現有GSM系統的變更降至最低限度，交遞作業的一部份包括建立用戶識別，並且一旦已實行交遞，就必須維護實體連接的發訊和資料機密(加密)。GSM 02.09.中提供用戶識別鑑認的定義及操作需求。

鑑認程序也用於設定加密鑰。因此，會在網路已建立用戶識別之後及頻道被加密之前，執行鑑認程序。為達成此目的需要兩項網路功能，即，鑑認程序本身，及系統之及鑑認鑰與加密鑰之管理。

請記住，理想情況是利用隨時可用的鑿通道(tunnelling)機制(在交遞情況與非交遞情況期間)，並且可能是單向或

雙向。其中一種鑿通道機制是所謂的ADDS (Application Data Delivery Service；應用資料傳遞服務)訊息及短資料叢發訊息(short data burst message)，用以在CDMA系統內無障礙傳遞GSM參數，這些參數通常不會被GSM基地控制器BSC檢查，然而是雙模式行動台所需的參數。一起使用ADDS訊息與資料叢發允許在網路的行動服務交換中心(MSC)或其他網路元件(例如，SMS、方位位置伺服器、OTASP)之間傳送通用封包承載。系統利用這項做法以在網路與行動台之間以端對端方式傳遞GSM資訊，而不需對CDMA BSCc或BTSc進行任何變更。

在圖2所示的網路配置中，ADDS訊息係用於將GSM交遞資料(例如，時序資訊和鑑認資料)透過BSCc從MSCc運送至行動台。然後，行動台使用所謂的MAP (Mobile Application Protocol；行動應用通訊協定)訊息，以將交遞資料運送至GSM網路中的MSCg。這只需要稍微改變MSCg，這能夠解譯MAP訊息中的資料，並且據此控制行動台。當然，也可使用其他的資料轉遞替代方案。

當行動台位於CDMA與GSM系統之間的邊界時(例如，在單元C2A中且正在接近單元C2B)，行動台開始交遞處理程序，其方式為將訊息回傳至MSCc，以向MSCc通知應將行動台交遞至GSM系統的狀況。

可使用單元資料庫(圖中未顯示)，以作為交遞程序的一部份。資料庫係用來將有關GSM網路的基本資訊提供給行動台，使行動台能夠視需要來執行CDMA MSC與GSM之間

的交遞。

在GSM系統中，有兩種可用的交遞類型，即，同步式與非同步式。為了易於實施，最好使用非同步式交遞。因此，告知行動台將以非同步交遞方式交遞至GSM。行動台接收到交遞命令後，行動台先將少許存取叢發(access burst)傳送至GSM基地台控制器BSCg，直到行動台接收到回傳至CDMA MSCc的MAP交遞訊息，以促使產生GSM鑑認資料，並且提供給行動台。GSM具有非同步交遞程序，其中資料叢發可協助BSCg獲取行動台的時序。因此，ADDS包含'動作時間'訊息，用以指定發生交遞的時間。只有在已接收到此資料後，行動台才會開始一般傳輸。

介於CDMA與GSM間之交遞的另一項問題為，CDMA和GSM鑑認係使用兩種不同的方法及金鑰。GSM與CDMA 1X的鑑認方法基本上相同，但是金鑰具有不同大小。CDMA 1X具有額外的程序，例如，唯一質問及計數(Unique Challenge and Count)方法，分別用於防止頻道攔截及重播攻擊。為了在GSM系統內使用的CDMA實體層，而不需要大幅修改GSM MSCg。應在CDMA實體層上重複利用GSM鑑認方法。這項做法的優點為，系統不需要支援兩種不同類型的鑑認中心、兩種類型的SIM卡等等。

鑑認程序係由系統與行動台之間的一連串交換所組成。系統將非可預測的號碼RAND傳輸至行動台。接著，行動台使用命為A3演算法的演算法來計算結果SRES(也稱為RAND號碼的簽名)。A3演算法使用RAND和個人用戶

鑑認鑰(Individual Subscriber Authentication Key) Ki來計算SRES。用戶鑑認鑰Ki係在客戶第一次訂購服務時配置，並且會被儲存在SIM(subscriber identity module；用戶識別模組)卡中及系統的主位置暫存器(Home Location Register；HLR)中。Ki是加密法中的私鑰，因此不會透過網路傳輸。最後，行動台將簽名SRES傳輸至系統，由系統測試其有效性。

請注意，指定使用的加密鑰和鑑認程序與交遞處理程序無關。附圖中的圖4顯示GSM MSC中如何實行鑑認。GSM中的鑑認鑰被稱為Ki，並且其長度為128位元。網路產生亂數(RAND)，其長度也是128位元。RAND和Ki被輸入至A3演算法，用以從輸入資料來計算32位元結果(SRES)。也會藉由空中訊息將 RAND 亂數傳輸至行動台。在GSM系統中，每個行動台都包含智慧卡，即，所謂的SIM(subscriber identity module；用戶識別模組)卡。GSM 11.11中指定標準的SIM鑑認命令。只有命令不會干擾GSM應用的正確運作時，才能執行這些命令。按照GSM 11.11中的定義，如果在行動台呼叫期間移除SIM，則會立即終止呼叫。

行動台中的SIM也會計算SRES，其方式為將A3演算法套用至所接收的RAND亂數及本機儲存的Ki複本。計算結果再次是SRES，並且應相同於系統的計算結果。因此，行動台將結果SRES傳送至網路，由網路比對於網路所計算的SRES值。如果SRES值都相同，則行動台是真的。在圖2所示的系統中，在空氣介面上使用ADDS訊息傳輸RAND亂數，並且傳回結果SRES。

命為A8的演算法也會使用SRES來計算加密鑰Kc。行動台中的SIM藉由GSM鑑認和加密演算法所產生的Kc金鑰被提供給CDMA實體層，以取代私用長碼遮罩(private long code mask，通常係使用CDMA CAVE演算法所產生)。64位元Kc金鑰被唯一對應至42位元私用長碼，並且當做"私用長碼遮罩"的基礎以提供語音隱私。整個CDMA訊息都會傳遞及解譯私用長碼遮罩，而且相同於CAVE演算法產生的私用長碼遮罩。在混合式CDMA/GSM網路內，使用這種語音隱私做法，可允許系統維持唯一鑑認中心及唯一SIM類型。

GSM在訊框層級執行加密。所有訊框都會使用訊框號碼及64位元Kc金鑰加密，其中金鑰係按照參考圖4的討論所衍生出。訊框號碼及Kc遮罩被套用至所有的訊框。在CDMA 1X系統中，使用42位元私用長碼來執行加密。在圖2所示的混合系統中，配合介於Kc金鑰與元私用長碼之間的對應演算法對應法，以使用Kc金鑰衍生出42位元私用長碼。這項對應法係在MSCc中執行，然接直接告知BSC欲使用的私用長碼。

ADDS作業允許在地面通訊網路元件(例如，MSC、SMS、PDC)與行動台之間無障礙傳遞服務。系統使用這項作業以將鑑認資訊RAND傳遞至MS，並且將SRES回傳至MSC。ADDS發訊(messaging)作業從MSCc移至BSCc，並且允許透過傳呼頻道以將資料傳送至行動台。ADDS傳遞(Transfer)作業從BSCc移至MSCc，並且允許透過接取頻道以將資料

從行動台傳送至網路。ADDS遞送(Deliver)作業從MSCc移至BSCc，或從BSCc移至MSCc，並且允許透過流量頻道以在行動台與網路之間傳送資料。ADDS參數已被定義為"ADDS使用者部份"(ADDS User Part)，其包含用於指示應用資料訊息格式的6位元"資料叢發類型"(Data Burst Type)。ADDS作業利用"ADDS使用者部份"參數以納入服務特有的資料。鑑認作業利用"ADDS使用者部份"以運載鑑認資料。所說明的系統使用新的"資料叢發類型"，名為"GSM-MAP鑑認"(GSM-MAP Authentication)，並且中行動台據此解譯。

請注意，每當接收端有用於儲存鑑認處理程序相關資訊的資料庫時，或接收端可存取該資料庫時，就可實施示範性具體實施例。可使用示範性具體實施例的處理器來實施與某方的某加密機制，及與另一方的另一加密機制。可實施示範性具體實施例的基本實施，而不需要中間資源的實體連接，因為會透過無線媒體進行各方的通訊。

熟知技藝人士應明白，配合本文所發表之具體實施例說明的各種圖解邏輯方塊、模組、電路及演算法步驟可實施為電子硬體、電腦軟體或其組合。各種圖解的組件、區塊、模組、電路及步驟已就其功能而論作一般性說明。視特定應用及影響整個系統的設計限制條件而定，將功能實施成硬體或軟體。熟知技藝人士應明白依據這些情況可交換硬體或軟體，以及如何針對每項特定應用，使實施說明的功能最理想。舉例而言，可使用專用積體電路(ASIC)、可程

式規劃邏輯裝置、離散閘極或電晶體邏輯、離散防火牆組件(如，暫存器及FIFO)、執行一組韌體指令的處理器、任何傳統可程式規劃軟體模組及微處理器，場可程式規劃閘極陣列(FPGA)或其他可程式規劃邏輯裝置(PLD)、或其任何的組合，以實施或執行配合本文所發表之具體實施例說明的各種圖解邏輯方塊、模組、電路及演算法步驟。處理器可能是微控制器，但是在替代方案中，處理器可能是任何傳統處理器、控制器、微控制器或狀態機器。軟體模組可駐存在RAM記憶體、快閃記憶體、ROM記憶體、EPROM記憶體、EEPROM記憶體、硬碟機、可抽換式磁碟、CD-ROM、DVD-ROM、暫存器或任何其他磁性或光學儲存媒體。熟習此項技術者應進一步明白，前面的整份說明書所提及的指令、命令、資訊、信號、位元、符號及晶片有利於以電壓、電流、電磁波、磁場或粒子、光場或粒子、或其任何組會來表示。

因此已參考較佳具體實施例來說明本發明，但是應知道，所討論的具體實施例僅僅是示範性具體實施例，並且具有適當知識及熟習此項技術者可進行各種變更和修改，而不會脫離如隨附申請專利範圍中所定義的本發明精神或範疇。

圖式代表符號說明

10	系統控制器和交換機
12,14,16,B1AtoB5A,B1BtoB5B	基地台
18,40,53	行動台

20a,22a,24a,20b,22b,24b	通訊鏈路
30	細胞式通訊網路
MSCc	劃碼多向近接(CDMA)行動中心
MSCg	GSM行動交換中心
C1AtoC5A	CDMA系統單元
C1BtoC5B	GSM系統單元
42,54	天線
44,55	雙工器
46,56	CDMA傳輸和接收鏈
48,57	GSM傳輸和接收鏈
40,50	基頻帶電路
52,59	控制器
34	系統間資料鏈路

肆、中文發明摘要

本發明揭示一種鑑認一行動台之方法，其中該行動台係從一由第一細胞式通訊系統中之第一行動交換控制台所控制之第一基地台接至一由第二、不同之細胞式通訊系統中之第二行動交換控制台所控制之第二基地台。該方法包括在該第二細胞式通訊系統產生一鑑認碼，其中產生之該鑑認碼是將一演算法套用至一指派給該第二細胞式通訊系統之該行動台的私鑰及由該第二細胞式通訊系統產生之一亂數的結果。在該第一細胞式通訊系統亦會產生一鑑認碼，其中產生之該鑑認碼是將一演算法套用至該私鑰及該亂數的結果。該第一細胞式通訊系統產生的該鑑認碼接著會置於一資料封包中傳輸至一行動台，並且從該行動台將該鑑認碼傳輸至該第二細胞式通訊系統。接著，將在該第一細胞式通訊系統產生的該鑑認碼比對於在該第二細胞式通訊系統產生的該鑑認碼。

伍、英文發明摘要

A method of authenticating a mobile station from a first base station in a first cellular communications system controlled by a first mobile switching control station to a second base station in a second, different cellular system controlled by a second mobile switching control station is described. The method comprises generating at the second cellular communication system an authentication code as the result of applying an algorithm to a private key assigned to the mobile station for the second cellular communications system and a random number generated by the second cellular communications system. An authentication code is also generated at the first cellular communication system as the result of applying an algorithm to the private key and the random number. The authentication code generated at the first cellular communication system is then transmitted to a mobile station in a data packet, and, from there, the authentication code is transmitted to the second cellular communication system. The authentication code generated at the first cellular communications system is then compared with the authentication code generated at the second cellular communications system.

拾壹、圖式

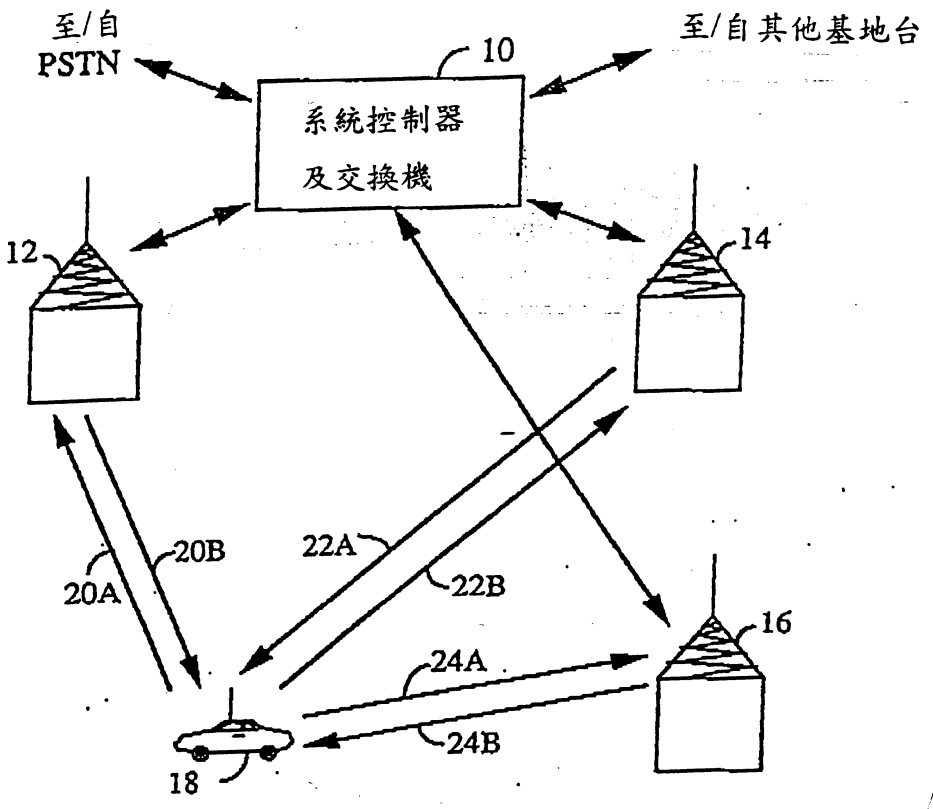

至/自
PSTN
10
至/自其他基地台
系統控制器
及交換機
12
14
16
18
20A
20B
22A
22B
24A
24B

圖 1

圖式頁

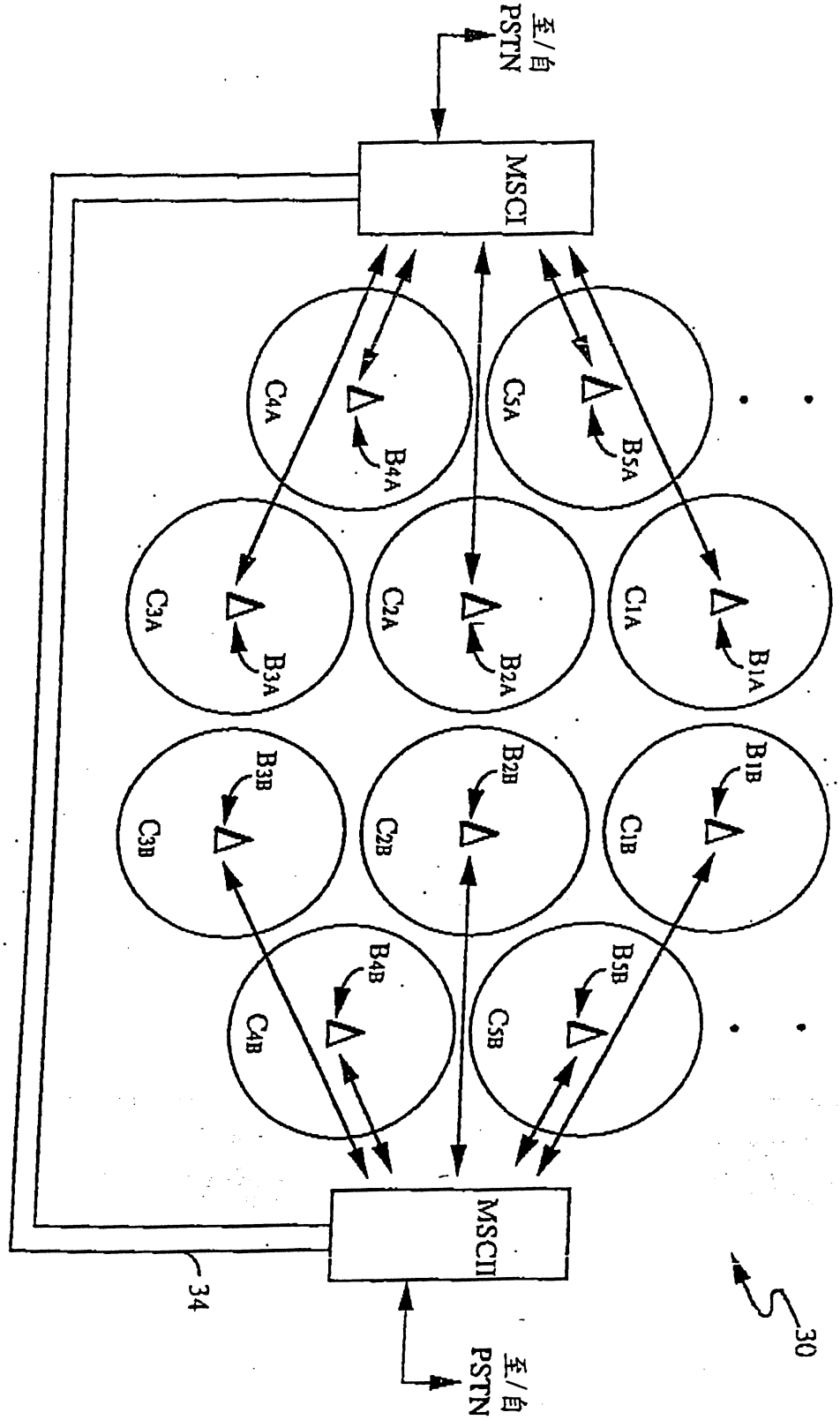

至/自
PSTN
MSCI
C4A
B4A
C5A
B5A
C3A
B3A
C2A
B2A
C1A
B1A
B3B
C3B
B2B
C2B
B1B
C1B
B4B
C4B
B5B
C5B
MSCII
至/自
PSTN
34
30

圖 2

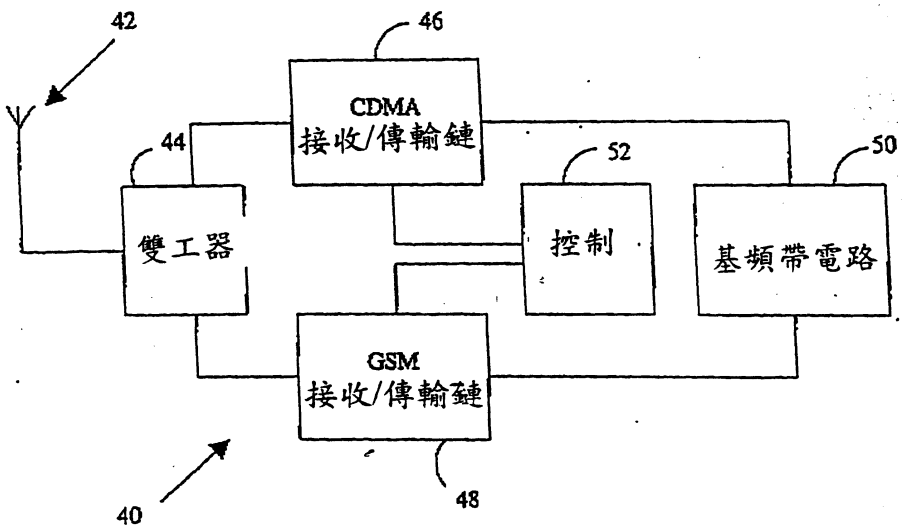


圖 3

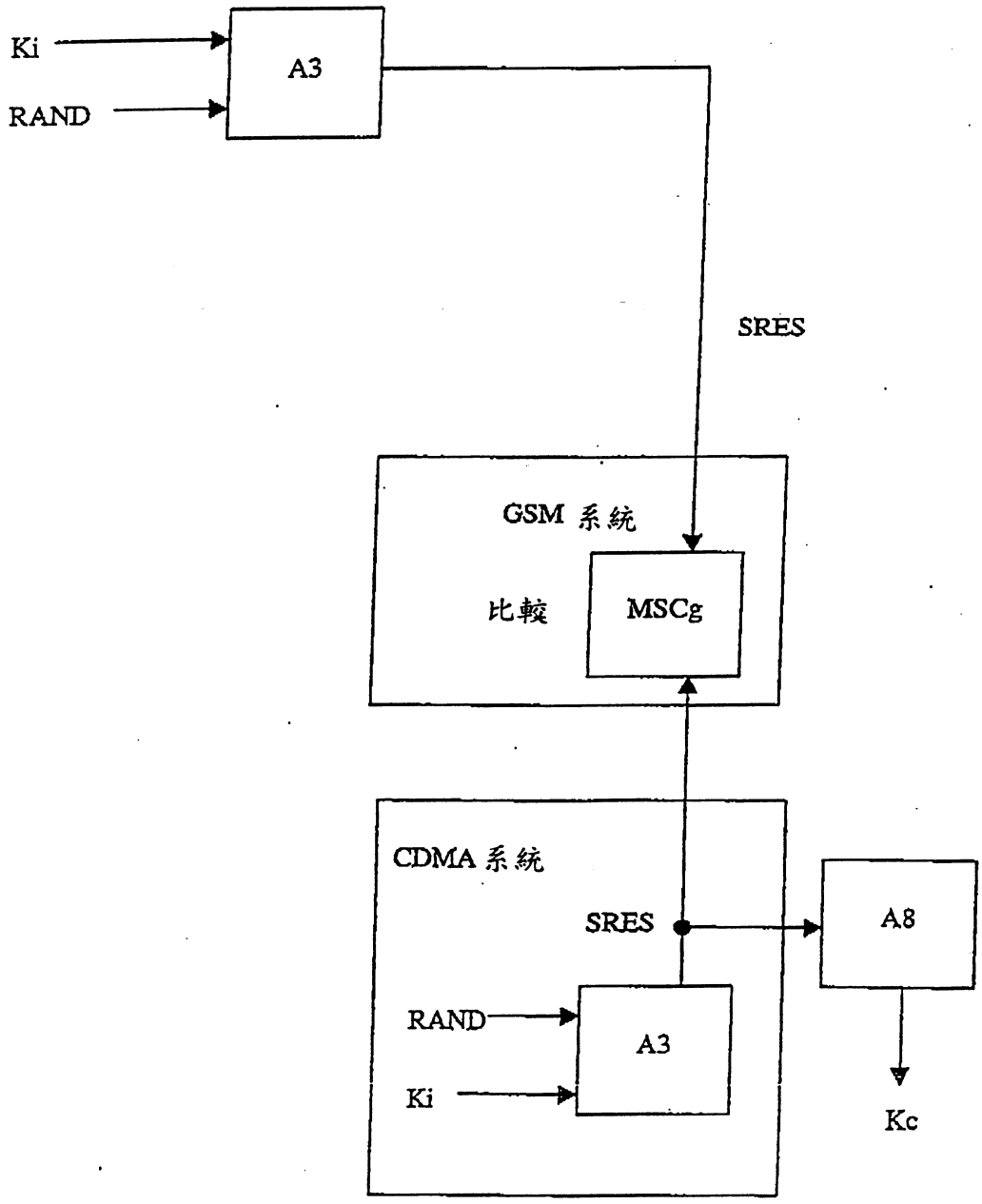


圖 4

圖式續頁

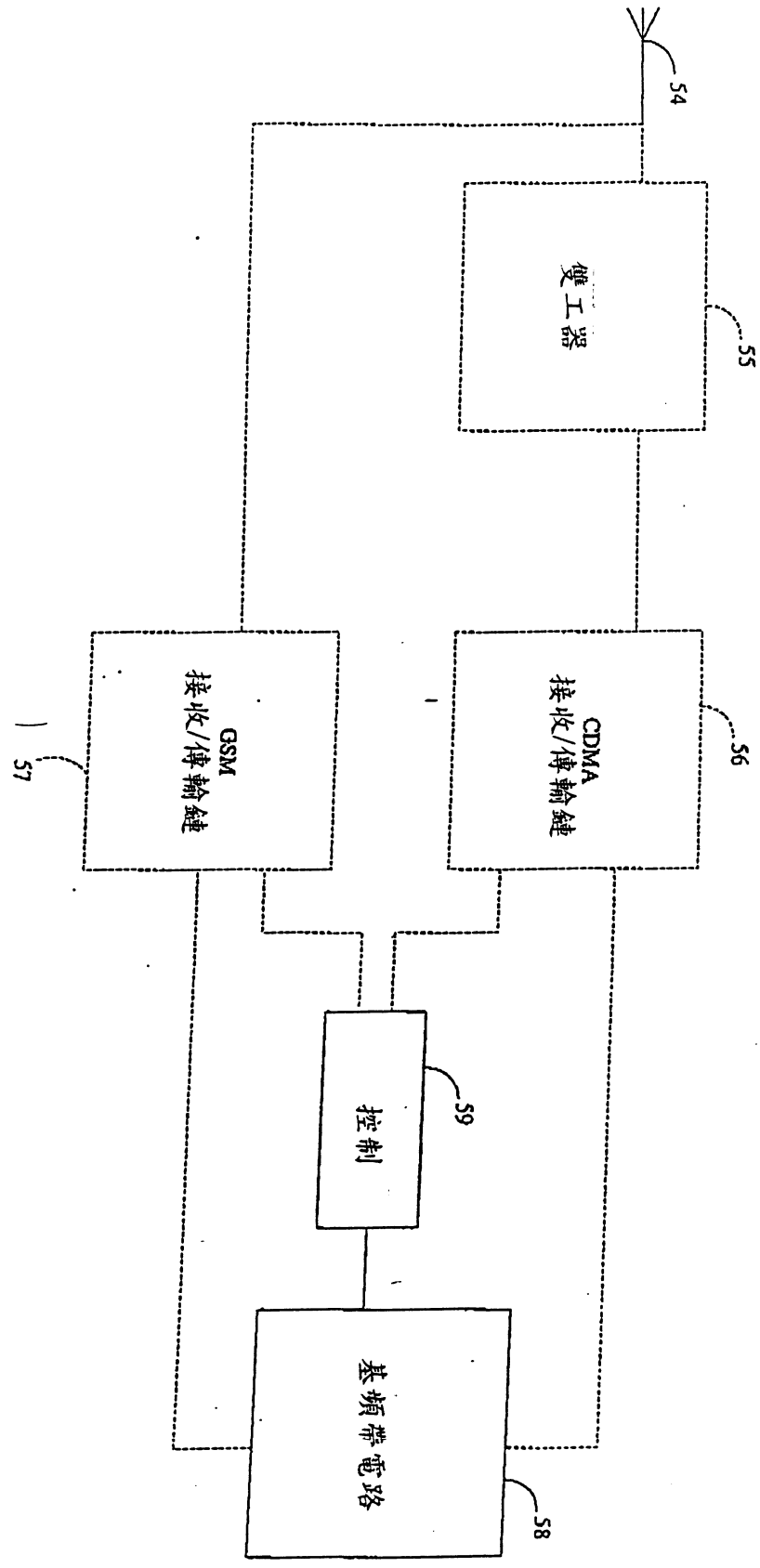


圖 5

陸、(一)、本案指定代表圖為：第 1 圖

(二)、本代表圖之元件代表符號簡單說明：

10	系統控制器和交換機
12	基地台
14	基地台
16	基地台
18	行動台
20A	通訊鏈路
20B	通訊鏈路
22A	通訊鏈路
22B	通訊鏈路
24A	通訊鏈路
24B	通訊鏈路

柒、本案若有化學式時，請揭示最能顯示發明特徵的化學式：

修正替換頁
98年6月6日

拾、申請專利範圍

1. 一種鑑認一行動台之方法，其中該行動台係從一由第一細胞式通訊系統中之第一行動交換控制台所控制之第一基地台接至一由第二、不同之細胞式通訊系統中之第二行動交換控制台所控制之第二基地台，該方法包括：

在該第二細胞式通訊系統產生一鑑認碼，其中產生之該鑑認碼是將一演算法套用至一指派給該第二細胞式通訊系統之該行動台的私鑰及由該第二細胞式通訊系統產生之一亂數的結果；

在該第一細胞式通訊系統產生一鑑認碼，其中產生之該鑑認碼是將一演算法套用至該私鑰及該亂數的結果；

將在該第一細胞式通訊系統產生之該鑑認碼以一資料封包傳輸至一行動台；

將在該第一細胞式通訊系統產生之該鑑認碼從該行動台傳輸至該第二細胞式通訊系統；以及

將在該第一細胞式通訊系統產生的該鑑認碼比對於在該第二細胞式通訊系統產生的該鑑認碼。

2. 如申請專利範圍第1項之方法，其中：

該第一細胞式通訊系統包括一劃碼多向近接(CDMA)系統；以及

該資料封包包括一ADDS訊息。

3. 如申請專利範圍第1項之方法，其中：

修正替換頁
年 月 日

該資料封包包含一指令，用以指示該行動台從該資料封包移除該鑑認碼；以及

該方法進一步包括，在該行動台從該資料封包移除該鑑認碼。

4. 如申請專利範圍第3項之方法，其中會在一不同資料封包中，將該鑑認碼傳輸至該第二細胞式通訊系統。

5. 如申請專利範圍第4項之方法，其中該第二細胞式通訊系統包括一GSM系統。

6. 如申請專利範圍第1項之方法，其中該第一細胞式通訊系統包括一由一第一行動交換控制台所控制之第一基地台，而該第二細胞式通訊系統包括一由一第二行動交換控制台所控制之第二基地台，該方法包括：

在該行動台量測一由該第一基地台所傳輸之信號的參數；

在該行動台量測一由該第二基地台所傳輸之信號的參數；

當該等參數到達一預先決定條件時，經由該第一基地台將一信號品質訊息從該行動台傳達至該第一行動交換控制台；

在該第一行動交換控制台產生該第二行動交換控制台之一頻道要求訊息的資訊；

將該資訊從該第一行動交換控制台傳達至該行動台；

在該行動台上，從來自該第一行動交換控制台的該

資訊產生該第二行動交換控制台之一頻道要求訊息；以及

將該頻道要求訊息從該行動台傳達至該第二行動交換控制台。

7. 如申請專利範圍第6項之方法，進一步包括在該第二行動交換控制台產生頻道資訊，用於識別該行動台在該第二行動交換控制台中的一頻道。

8. 如申請專利範圍第7項之方法，進一步包括在該識別頻道中，建立介於該行動台與該第二基地台之間的通訊。

9. 如申請專利範圍第8項之方法，進一步包括切斷介於該行動台與該第二基地台之間的通訊。

10. 如申請專利範圍第6項之方法，其中該參數對應於信號強度。

11. 一種於一系統中之裝置，該系統具有一行動台，該行動台從一由第一細胞式通訊系統中之第一行動交換控制台所控制之第一基地台接至一由第二、不同之細胞式通訊系統中之第二行動交換控制台所控制之第二基地台，該裝置包括：

鑑認碼產生構件，用於在該第二細胞式通訊系統產生一鑑認碼，其中產生之該鑑認碼是將一演算法套用至一指派給該等第二細胞式通訊系統之該行動台的私鑰及該第二細胞式通訊系統產生之一亂數的結果；

鑑認碼產生構件，用於在該第一細胞式通訊系統產生一鑑認碼，其中產生之該鑑認碼是將一演算法套用

至該私鑰及該亂數的結果；

傳輸構件，用於在一資料封包中，將在該第一細胞式通訊系統產生之該鑑認碼傳輸至一行動台；

傳輸構件，用於將在該第一細胞式通訊系統產生之該鑑認碼從該行動台傳輸至該第二細胞式通訊系統；以及

比較構件，用於將在該第一細胞式通訊系統產生的該鑑認碼比對於在該第二細胞式通訊系統產生的該鑑認碼。

12. 如申請專利範圍第11項之裝置，其中：

該第一細胞式通訊系統包括一CDMA系統；以及

該資料封包包括一ADDS訊息。

13. 如申請專利範圍第11項之裝置，其中：

該資料封包包含一指令，用以指示該行動台從該資料封包移除該鑑認碼；以及

該裝置進一步包括移除構件，用於在該行動台從該資料封包移除該鑑認碼。

14. 如申請專利範圍第13項之裝置，其中會在一不同資料封包中，將該鑑認碼傳輸至該第二細胞式通訊系統。

15. 如申請專利範圍第14項之裝置，其中該第二細胞式通訊系統包括一GSM系統。